

Biztonság és védelem az informatikában

2. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

Felhasznált programok:

WindowsPortableApps, TcpView, ProcessExplorer, AutoRuns, WireShark

2021.02.18

Bot, Worm behatoló detektálása

Miután a leírtak szerint letöltöttem a WindowsPortableApps, tcpView, ProcessExplorer és AutoRuns alkalmazásokat, és a licenseket is jóváhagytam az Autoruns programot indítottam el.

Ezen alkalmazás segítségével a jelenleg futó alkalmazásokat tudom megtekinteni:

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2020. 07. 14. 12:13	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1909. 05. 14. 1:57	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 17. 7:53	
<input checked="" type="checkbox"/> Vanguard	Vanguard tray notification.	(Verified) Riot Games, Inc.	c:\program files\riot vanguard\vgtray....	2021. 01. 22. 21:31	
<input checked="" type="checkbox"/> RTHDVBg_Dolby	HD Audio Background Process	(Verified) Realtek Semiconductor Corp.	c:\program files\realtek\audio\hda\vr...	2016. 08. 24. 8:13	
<input checked="" type="checkbox"/> RTHDVCPL	Realtek HD Audio Manager	(Verified) Realtek Semiconductor Corp.	c:\program files\realtek\audio\hda\vr...	2016. 09. 26. 6:48	
<input checked="" type="checkbox"/> RZSurroundHelper		(Verified) Razer USA Ltd.	c:\windows\system32\rzsurroundhel...	2019. 09. 18. 5:01	
<input checked="" type="checkbox"/> THX051eHelper		(Verified) Razer USA Ltd.	c:\program files (x86)\vazer\apo051e...	2019. 09. 18. 5:53	
<input checked="" type="checkbox"/> THX22adHelper		(Verified) Razer USA Ltd.	c:\program files (x86)\vazer\thxvad\...	2019. 09. 18. 5:55	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2021. 01. 23. 21:37	
<input checked="" type="checkbox"/> Dropbox	Dropbox	(Verified) Dropbox, Inc	c:\program files (x86)\dropbox\client\...	1995. 02. 14. 6:37	
<input checked="" type="checkbox"/> LogMeIn Hamachi Ui	Hamachi Client Application	(Verified) LogMeIn, Inc.	d:\programs\hamachi\hamachi-2-ui.e...	2019. 04. 02. 15:58	
<input checked="" type="checkbox"/> RazerCortex	CortexLauncher.exe	(Verified) Razer USA Ltd.	d:\programs\vazer cortex\cortexlaunc...	2020. 02. 05. 9:20	
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\j...	2020. 12. 09. 15:24	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 15. 16:03	
<input checked="" type="checkbox"/> ApacheTomcatMonitor9...			File not found: C:\Program Files\Apa...		
<input checked="" type="checkbox"/> CCXProcess	CCXProcess	(Verified) Adobe Inc.	c:\program files (x86)\adobe\adobe ...	2019. 10. 22. 17:25	
<input checked="" type="checkbox"/> CiscoMeetingDaemon	Cisco Webex Meeting	(Verified) Cisco WebEx LLC	c:\users\bgabe\appdata\local\webe...	2021. 02. 05. 14:55	
<input checked="" type="checkbox"/> com.blitz.app	Blitz	(Verified) Swift Media Entertainment, I...	c:\users\bgabe\appdata\local\progr...	2021. 01. 23. 1:18	
<input checked="" type="checkbox"/> com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Applicati...	c:\users\bgabe\appdata\local\micro...	2020. 10. 02. 13:48	
<input checked="" type="checkbox"/> Discord	Update	(Verified) Discord Inc.	c:\users\bgabe\appdata\local\disco...	2020. 06. 01. 21:58	
<input checked="" type="checkbox"/> EpicGamesLauncher	EpicGamesLauncher	(Verified) Epic Games Inc.	d:\programs\epic games\launcher\p...	2021. 02. 16. 14:42	
<input checked="" type="checkbox"/> MLWapp	Video Wallpaper	(Not verified) mylive wallpapers.com	d:\downloads\mlwapp\mlwapp.exe	2019. 11. 29. 8:45	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\bgabe\appdata\local\micro...	1958. 02. 05. 12:59	
<input checked="" type="checkbox"/> ProtonVPN	ProtonVPN	(Verified) ProtonVPN AG	d:\programs\proton\protonvpn.exe	2020. 07. 22. 12:05	
<input checked="" type="checkbox"/> RzAppEngine	Razer AppEngine	(Verified) Razer USA Ltd.	c:\program files\vazer\rzappengine\rz...	2018. 08. 05. 6:00	
<input checked="" type="checkbox"/> Steam	Steam Client Bootstrapper	(Verified) Valve	d:\programs\steam\steam.exe	2021. 02. 13. 0:23	
<input checked="" type="checkbox"/> Synapse3	Razer Synapse 3	(Verified) Razer USA Ltd.	d:\programs\synapse3\wpfui\framew...	1903. 04. 23. 14:00	
<input checked="" type="checkbox"/> uTorrent	µTorrent	(Verified) BitTorrent Inc	c:\users\bgabe\appdata\roaming\ut...	2020. 12. 09. 1:05	
<input checked="" type="checkbox"/> Web Companion	Web Companion	(Verified) LAVASOFT SOFTWARE C...	c:\program files (x86)\lavasoft\web c...	2021. 02. 12. 14:15	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				2021. 02. 23. 8:58	
<input checked="" type="checkbox"/> Application Restart #3	Razer AppEngine	(Verified) Razer USA Ltd.	c:\program files\vazer\rzappengine\rz...	2018. 08. 05. 6:00	

Ready. Signed Windows Entries Hidden.

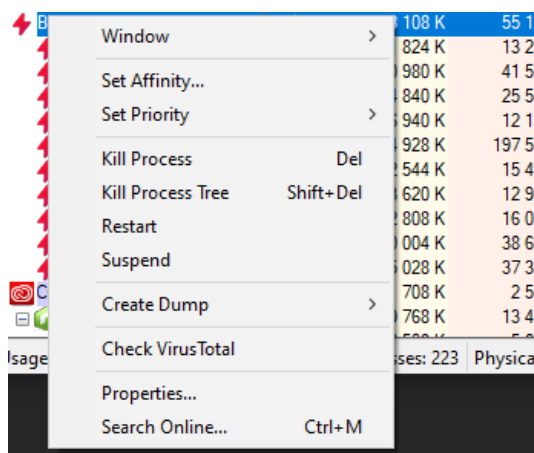
A részletesebb vizsgálathoz ProcessExplorer-t használtam, melyet a feladat leírásban megjelölt linken töltöttem le.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-CNLF766\bgabe]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Registry		8 020 K	49 360 K	120			
System Idle Process	70.07	60 K	8 K	0			
System	2.16	208 K	4 756 K	4			
System Interrupts	1.27	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		1 152 K	896 K	484			
Memory Compression	0.19	2 820 K	220 044 K	2624			
csrss.exe	< 0.01	2 024 K	5 224 K	688			
wininit.exe		1 760 K	6 180 K	772			
services.exe	0.37	7 156 K	12 932 K	848			
svchost.exe		908 K	3 472 K	988	Windows-szolgáltatások gaz...	Microsoft Corporation	
svchost.exe	0.01	26 340 K	33 156 K	1008	Windows-szolgáltatások gaz...	Microsoft Corporation	
WmiPrvSE.exe	0.02	2 992 K	9 116 K	3792			
dllhost.exe		3 744 K	9 996 K	9908			
usocoreworker.exe		85 528 K	13 556 K	13244			
StartMenuExperienceHost.exe		25 164 K	15 844 K	8976			
RuntimeBroker.exe		6 260 K	14 580 K	12432	Runtime Broker	Microsoft Corporation	
SearchUI.exe	Susp...	209 892 K	8 884 K	17136	Search and Cortana applicati...	Microsoft Corporation	
SettingSyncHost.exe	< 0.01	11 920 K	6 968 K	15708	Host Process for Setting Syn...	Microsoft Corporation	
RuntimeBroker.exe	< 0.01	14 180 K	17 448 K	10396	Runtime Broker	Microsoft Corporation	
YourPhone.exe	Susp...	45 396 K	492 K	5904	YourPhone	Microsoft Corporation	
ShellExperienceHost.exe	0.01	35 476 K	61 400 K	3016	Windows Shell Experience H...	Microsoft Corporation	
RuntimeBroker.exe		5 160 K	20 456 K	10596	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe		6 512 K	16 668 K	15212	Runtime Broker	Microsoft Corporation	
LockApp.exe	Susp...	32 596 K	9 904 K	16284	LockApp.exe	Microsoft Corporation	
RuntimeBroker.exe		8 140 K	12 224 K	13116	Runtime Broker	Microsoft Corporation	
dllhost.exe		5 888 K	12 292 K	6500	COM Surrogate	Microsoft Corporation	
RuntimeBroker.exe		2 700 K	12 820 K	10612	Runtime Broker	Microsoft Corporation	
CompPkgSrv.exe		2 488 K	8 748 K	8108	Component Package Suppor...	Microsoft Corporation	
ApplicationFrameHost.exe		5 124 K	13 848 K	18136	Application Frame Host	Microsoft Corporation	

CPU Usage: 29.93% | Commit Charge: 62.70% | Processes: 221 | Physical Usage: 85.45%



Lehetőségünk van leállítani újraindítani elindítani, illetve felfüggeszteni az alkalmazásokat.

Gyanús programok esetén még esélyünk van egy Check VirusTotal lehetőségre is mely során a programról készített egyedi hash-t vírus keresőket tartalmazó weblapra küldi el, majd megtekinthetjük az eredményeket a legutolsó sorban lévő '[0/75](#)'-re kattintva.

Blitz.exe	0.31	70 992 K	64 680 K	5096	Blitz	Blitz, Inc.	0/75
-----------	------	----------	----------	------	-------	-------------	----------------------

0 / 57

Community Score

?

Community Score

✓

No engines detected this file

86534b4c78fe27651d2e2a03a258d0da3166d5d4e9762650ef62c4c3466cdcc1

Blitz.exe

104.80 MB

Size

2021-02-22 19:17:44 UTC

18 hours ago

EXE

overby

peexe

signed

DETECTION	DETAILS	COMMUNITY
Acronis	✓ Undetected	Ad-Aware ✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3 ✓ Undetected
Alibaba	✓ Undetected	ALYac ✓ Undetected
Antiy-AVL	✓ Undetected	SecureAge APEX ✓ Undetected
Arcabit	✓ Undetected	Avast ✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu ✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta ✓ Undetected
Bkav Pro	✓ Undetected	CAT-QuickHeal ✓ Undetected
ClamAV	✓ Undetected	CMC ✓ Undetected
Comodo	✓ Undetected	CrowdStrike Falcon ✓ Undetected
Cybereason	✓ Undetected	Cyren ✓ Undetected
DrWeb	✓ Undetected	eGambit ✓ Undetected
Emsisoft	✓ Undetected	eScan ✓ Undetected
FSFT-NOD32	✓ Undetected	F-Secure ✓ Undetected

Egy futó alkalmazásra jobb gombbal kattintva majd a properties menüpontot kiválasztva Részletes információt kapunkhatunk róla. Ilyenek például: a verziószám, a program indulási helye, adott user azonosító, aki használja és a futtatás kezdetének időpontja. A Performance fülön keresztül pedig további információkhoz juthatunk a processzor, a virtuális, illetve fizikai memória adatairól, valamint a I/O műveletekről.

Blitz.exe:5096 Properties

Threads

TCP/IP

Security

Environment

Strings

Image

Performance

Performance Graph

GPU Graph

Image File

Blitz

Version: 1.13.127.1270

Build Time: Sat Jan 23 01:18:26 2021

Path: C:\Users\lgabe\AppData\Local\Programs\Blitz\Blitz.exe

Explore

Command line: "C:\Users\lgabe\AppData\Local\Programs\Blitz\Blitz.exe" --autostart

Current directory: C:\Windows\System32\

Autostart Location: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\cc

Explore

Parent: explorer.exe(3400)

User: DESKTOP-CNL7F66\lgabe

Started: 8:57:57 2021. 02. 23. Image: 32-bit

Comment:

VirusTotal:

Submit

Data Execution Prevention (DEP) Status: Enabled (permanent)

Address Space Load Randomization: Bottom-Up

Control Flow Guard: Enabled

Enterprise Context: N/A

Verify

Bring to Front

Kill Process

OK

Cancel

Blitz.exe:5096 Properties

Threads

TCP/IP

Security

Environment

Strings

Image

Performance

Performance Graph

GPU Graph

CPU

Priority 8

Kernel Time 0:01:56.234

User Time 0:01:10.140

Total Time 0:03:06.375

Cycles 675 677 674 423

Virtual Memory

Private Bytes 67 680 K

Peak Private Bytes 78 860 K

Virtual Size 670 928 K

Page Faults 533 666

Page Fault Delta 0

Physical Memory

Memory Priority 5

Working Set 54 540 K

WS Private 21 644 K

WS Shareable 32 884 K

WS Shared 32 884 K

Peak Working Set 100 768 K

I/O

I/O Priority Normal

Reads 261 517

Read Delta 0

Read Bytes Delta 0

Writes 303 140

Write Delta 0

Write Bytes Delta 0

Other 2 439 007

Other Delta 4

Other Bytes Delta 122 B

Handles

Handles 1 031

Peak Handles 1 031

GDI Handles 28

USER Handles 59

OK

Cancel

A harmadik TcpView melyel az éppen futó alkalmazások hálózati használati tulajdonságát tudom elemezni. A state oszlopban a státusz tulajdonság szerepel mely azt jelzi, hogy a program vár a kapcsolódásra 'Listening' vagy pedig már kapcsolódott 'Established'.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets
chrome.exe	5208	UDP	DESKTOP-CNL7F...	5353	*	*		
chrome.exe	5208	UDPV6	desktop-cnl7f66...	5353	*	*		
chrome.exe	13680	TCP	desktop-cnl7f66...	53878	172.217.218.189	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66...	53952	bud02s26-in-f14.1...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66...	53959	zrh04s05-in-f99.1e...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66...	53969	prg02s12-in-f22.1e...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66...	54004	edge-star-mini-shv...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66...	54005	bud02s24-in-f238...	https	ESTABLISHED	
Discord.exe	5388	TCP	DESKTOP-CNL7F...	6463	DESKTOP-CNL7F...	0	LISTENING	
Discord.exe	19068	TCP	desktop-cnl7f66...	53407	162.159.137.234	https	ESTABLISHED	
Discord.exe	19068	TCP	desktop-cnl7f66...	53946	162.159.134.234	https	ESTABLISHED	
Discord.exe	5388	UDP	DESKTOP-CNL7F...	63156	*	*		
hamachi-2.exe	9024	TCP	desktop-cnl7f66...	61994	95.172.70.132	12975	ESTABLISHED	
hamachi-2.exe	9024	UDP	desktop-cnl7f66...	58703	*	*		
hamachi-2.exe	9024	UDP	DESKTOP-CNL7F...	58704	*	*		
lsass.exe	864	TCP	DESKTOP-CNL7F...	49664	DESKTOP-CNL7F...	0	LISTENING	
lsass.exe	864	UDPV6	desktop-cnl7f66...	49664	desktop-cnl7f66...	0	LISTENING	
OriginWebHel...	8552	TCP	DESKTOP-CNL7F...	3213	DESKTOP-CNL7F...	0	LISTENING	
OriginWebHel...	8552	UDP	DESKTOP-CNL7F...	49156	*	*		
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:1]	61934	[0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:1]	61937	[0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:1]	61940	[0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:1]	61943	[0:0:0:0:0:0:1]	5426	ESTABLISHED	
SearchUI.exe	17136	TCP	desktop-cnl7f66...	50264	152.199.19.161	https	CLOSE_WAIT	
services.exe	848	TCP	DESKTOP-CNL7F...	49683	DESKTOP-CNL7F...	0	LISTENING	
services.exe	848	UDPV6	desktop-cnl7f66...	49683	desktop-cnl7f66...	0	LISTENING	

Endpoints: 151 Established: 43 Listening: 30 Time Wait: 9 Close Wait: 1

Végül már csak a wireShark maradt kipróbálásra.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
89881	212.301315	52.115.130.57	192.168.1.67	UDP	175	3479 → 50003 Len=133
89882	212.305537	213.163.93.18	192.168.1.67	UDP	1149	50001 → 63126 Len=1107
89883	212.308131	52.115.130.57	192.168.1.67	UDP	120	3481 → 50042 Len=78
89884	212.308428	52.115.130.57	192.168.1.67	UDP	101	3481 → 50042 Len=59
89885	212.308428	52.115.130.57	192.168.1.67	UDP	104	3481 → 50042 Len=62
89886	212.308428	52.115.130.57	192.168.1.67	UDP	136	3481 → 50042 Len=94
89887	212.308428	52.115.130.57	192.168.1.67	UDP	136	3481 → 50042 Len=94
89888	212.309026	52.115.130.57	192.168.1.67	UDP	120	3480 → 50028 Len=78
89889	212.309345	52.115.130.57	192.168.1.67	UDP	742	3480 → 50028 Len=700
89890	212.309346	52.115.130.57	192.168.1.67	UDP	742	3480 → 50028 Len=700
89891	212.310868	192.168.1.67	213.163.93.18	UDP	94	63126 → 50001 Len=52

> Frame 9782: 108 bytes on wire (864 bits), 108 captured (864 bits) on interface \Device\NPF_{406DCA01-3BDD-42F6-AAAA-1E569FEA93F8}

> Ethernet II, Src: Sagemcom_fc:e2:b5 (34:db:9c:fc:e2:b5), Dst: RivetNet_22:16:93 (9c:b6:d0:22:16:93)

> Internet Protocol Version 4, Src: 193.6.5.33, Dst: 192.168.1.67

> Transmission Control Protocol, Src Port: 21, Dst Port: 54774, Seq: 1, Ack: 1, Len: 54

> File Transfer Protocol (FTP)

[Current working directory:]

0000 9c b6 d0 22 16 93 34 db 9c fc e2 b5 08 00 45 00 ...4...E

0010 00 5e 20 12 40 00 36 06 9c 75 c1 06 05 21 c0 a8 ...6...u...

0020 01 43 00 15 d5 f6 6d 06 26 f6 8e d1 02 4a 50 18 ...C...m: &...JP

0030 72 10 a2 f9 00 00 32 32 30 20 50 72 6f 46 54 50 ...22 0 ProFTP

0040 44 20 31 2e 33 2e 35 62 20 53 65 72 76 65 72 20 ...1.3.5b Server

0050 28 68 65 72 61 29 20 5b 3a 3a 66 66 66 66 3a 31 (hera) [:ffff:1

0060 39 33 2e 36 2e 35 2e 33 33 5d 0d 0a 93.6.5.33]...

wireshark_Wi-FiB8FC20.pcapng

Packets: 90089 · Displayed: 90089 (100.0%)

Profile: Default

A leírtak szerint a Commanderrel bejelentkeztem a Miskolci egyetem ftp-szerverére és ki capture-öltem a bejelentkezési információkat.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
9782	20.038993	193.6.5.33	192.168.1.67	FTP	108	Response: 220 ProFTPD 1.3.5b Server (hera) [::ffff:193.6.5.33]
9789	20.047696	192.168.1.67	193.6.5.33	FTP	68	Request: OPTS UTF8 ON
9798	20.067686	193.6.5.33	192.168.1.67	FTP	74	Response: 200 UTF8 set to on
11846	23.747987	192.168.1.67	193.6.5.33	FTP	69	Request: USER baranyi2
11877	23.762915	193.6.5.33	192.168.1.67	FTP	90	Response: 331 Password required for baranyi2
13479	26.700248	192.168.1.67	193.6.5.33	FTP	72	Request: PASS
13493	26.720692	193.6.5.33	192.168.1.67	FTP	83	Response: 230 User baranyi2 logged in

< >

> Frame 9782: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface \Device\NPF_{4D6DCA01-38DD-42F6-AAAA-1E569FEA93F8}

> Ethernet II, Src: Sagemcom_fc:e2:b5 (34:db:9c:fc:e2:b5), Dst: RivetNet_22:16:93 (9c:b6:d0:22:16:93)

> Internet Protocol Version 4, Src: 193.6.5.33, Dst: 192.168.1.67

> Transmission Control Protocol, Src Port: 21, Dst Port: 54774, Seq: 1, Ack: 1, Len: 54

> File Transfer Protocol (FTP)

[Current working directory:]

< >

```
0000  9c b6 d0 22 16 93 34 db 9c fc e2 b5 08 00 45 00  ...4. ....E
0010  00 5e 20 12 40 00 36 06 9c 75 c1 06 05 21 c0 a8  ^..@.6. .u...!
0020  01 43 00 15 d5 f6 6d 06 26 f6 8e d1 02 4a 50 18  .C...m. &....JP
0030  72 10 a2 f9 00 00 32 32 30 20 50 72 6f 46 54 50  r.....22 0 ProFTP
0040  44 20 31 2e 33 2e 35 62 20 53 65 72 76 65 72 20  D 1.3.5b Server
0050  28 68 65 72 61 29 20 5b 3a 3a 66 66 66 66 3a 31  (hera) [ ::ffff:1
0060  39 33 2e 36 2e 35 2e 33 33 5d 0d 0a 93.6.5.3 3 ]...
```

Wi-Fi: <live capture in progress> | Packets: 55363 · Displayed: 7 (0.0%) | Profile: Default